At the Intersection of Broadband and Transportation

Brian Isle
Senior Fellow
Adventium Labs
&
University of Minnesota

612-716-5604
brian.isle@adventiumlabs.com

Agenda

- Cars, Computers & Networks.
- We are all connected.
- What do the bad guys want?
- Approach for securing the future.

Goal of the presentation: Raise your awareness of transportation security issues, scare you a bit, & give you some hope.

Cars: Basically a computer with four wheels.

CARS, COMPUTERS & NETWORKS

Marvels of Computing & Wireless Network

#4: 2014 Toyota Prius

"With its Safety Connect system, Bluetooth, remote keyless entry, proprietary radio and a cellular network, Prius has a large potential remote attack surface.

The brakes and steering are on the same network as the Bluetooth, posing a risk. Features like the self-parking and pre-collision systems could possibly be compromised."

http://www.bankrate.com/finance/auto/most-hackable-cars-1.aspx#ixzz3UknASEFx

What Could be Exploited?

BMW Hack: the auto industry's big cyber-security warning sign

"A cyber-security hole that left more than two million BMWs vulnerable …"

"German researchers spoofed a cell-phone station and sent fake messages to a SIM card within a BMW's telematics system. … Other researchers have demonstrated it's possible to hack into a car and control its critical functions, but what separates this latest exploit from others is that it was conducted remotely."

http://www.autoblog.com/2015/02/06/bmw-hack-cyber-security-warning-feature-video/

Robocar Will Only Up-The-Ante

BMW's Chinese Robocar Tests Will Use Baidu's Maps

"BMW is collaborating with the Chinese search-engine giant Baidu to provide its experimental self-driving cars with maps of select Chinese roads"

Photo: Krzysztof Dydynski/Getty Images

"…self-driving car can not manage without digital maps…. maps that show the roads and what's alongside them, warts and all. … every exit ramp, every driveway, and every curb. …. no amount of memory can free robotic cars from the need to talk to the road and to each other." http://spectrum.ieee.org/cars-that-think/transportation/self-driving/bmw-robocars-in-china-w/?utm_source=techalert&utm_medium=email&utm_campaign=100214

Robocar will be a sensor that captures realtime data on traffic, road conditions, and what the driver/passengers are doing while in route.

“Robotic Taxis Could Slash Fares”

“When driverless taxis are at our beck and call, a lot of people will give up the chore of driving and parking, streets will be less crowded, and commuting times will drop, say proponents of automated automobiles.”

http://spectrum.ieee.org/cars-that-think/transportation/self-driving/robotic-taxis-could-slash-fares-in-austin-texas

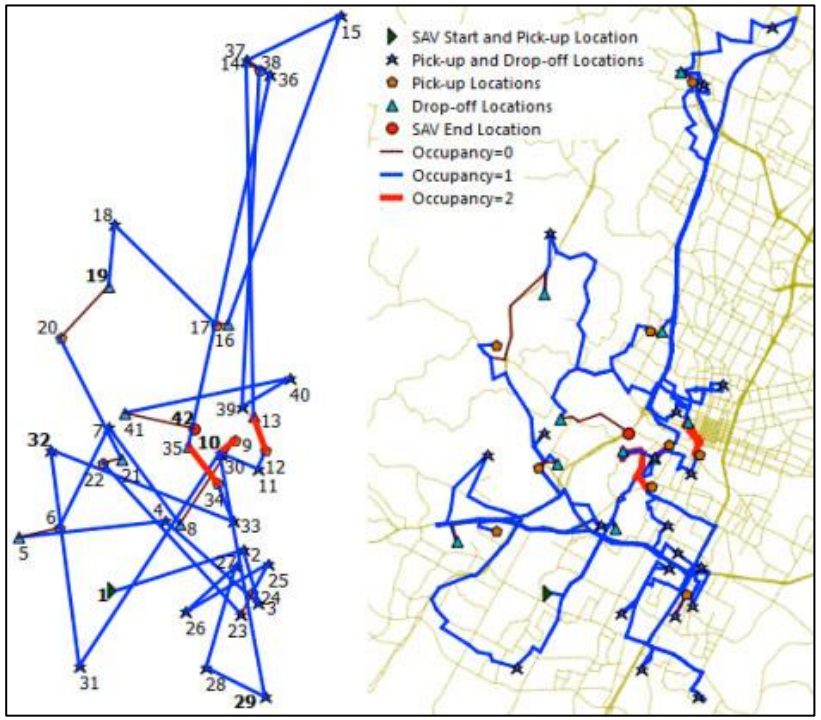


Image: The University of Texas at Austin

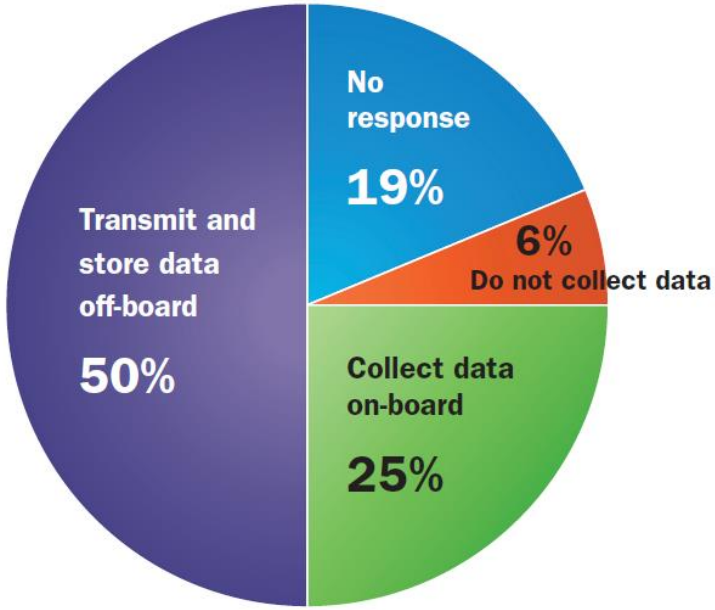
The Robo Taxi needs to be paid. So Robo Taxi knows who you are, your credit card, where you started and where you are going. This will be conveyed on broadband. Any worries?

Most Car Manufactures Collect Personal Data

"Manufacturers use personal vehicle data in various ways, often vaguely to "improve the customer experience" ….."

Tracking & Hacking: Security & Privacy Gaps Put American Drivers at Risk, February 2015

www.markey.senate.gov



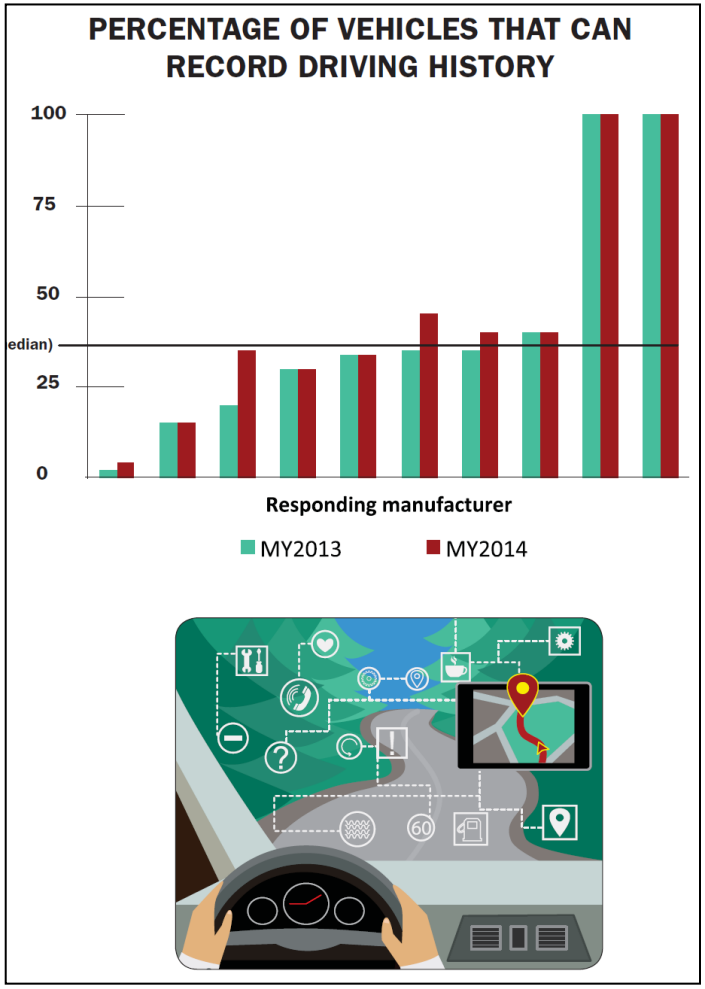
PERCENTAGE OF AUTOMOBILE MANUFACTURERS THAT COLLECT AND TRANSMIT DRIVING HISTORY DATA

Your car and the manufacturer have a lot of your personnel data.

Data Tells Where You Are & How Fast You Got There

- Physical location recorded at regular intervals;
  - Previous destinations entered into navigation system;
  - Last location parked.
- System settings for event data recorder (EDR) devices
  - Potential crash events, such as sudden changes in speed
  - Status of steering angle, brake application,
  - seat belt use, and air bag deployment;
  - Fault/error codes in electronic systems.
- Operational data
  - Vehicle speed;
  - Direction/heading of travel;
  - Distances and times traveled;
  - Car operational data.

Markey study 2015



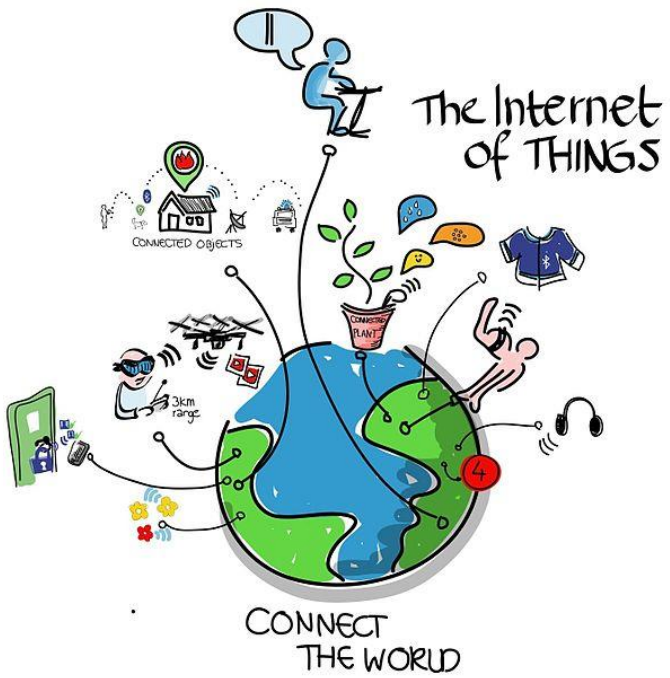
What could a bad guy or an insurance lawyer do with the data?

WE ARE ALL CONNECTED

Internet of “every”-Thing

Internet of Things is the network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment. (Gartner)

- Any device that is IP addressable, has CPU, memory, & firmware. (BAI)
- Often Edge-devices



http://en.wikipedia.org/wiki/Internet_of_Things#mediaviewer/File:Internet_of_Things.jpg

Everything from your toothbrush to your speedometer will be IoT.

Can't We Just Hide? - NO

SHODAN – Computer Search Engine: Search for computers based on software, geography, operating system, IP address and more. *www.**shodan**hq.com/*

Scariest Search Engine on the Internet Just Got Scarier

- Project SHINE (SHodan INtelligence Extraction) from Bob Radvanovsky and Jake Brodsky of Infracritical. Its purpose is to use Shodan to locate SCADA devices connected to the internet.
- "The average number of new SCADA/ICS devices found every day is between 2000 and 8000. So far we have collected over 1,000,000 unique IP addresses that appear to belong to either SCADA and control systems devices or related software products."

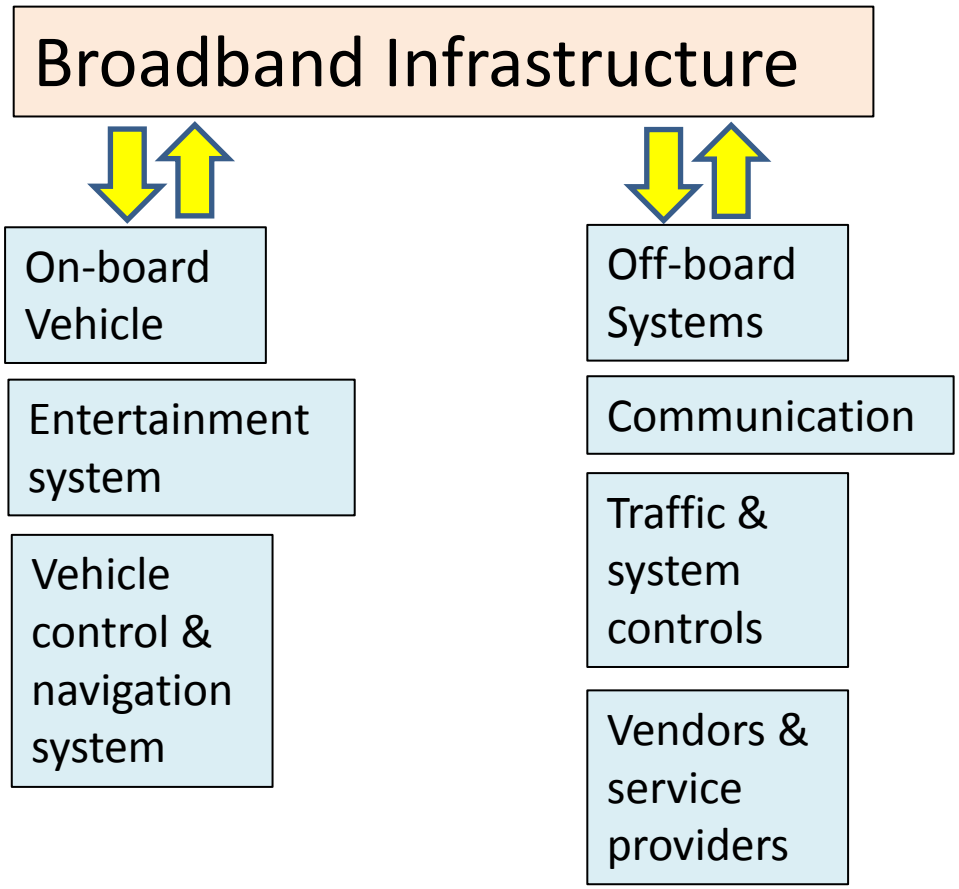
http://www.infosecurity-magazine.com/news/scariest-search-engine-on-the-internet-just-got/

Security by obscurity is not an option – AND – and the strategy of depending on air gap is a myth.

Connectivity: A Simplified View

Think broadly: planes, trains, & automobiles

- All have control systems
- Traffic & system controls are "SCADA"



Why Protect Control Systems

Source: Dr. John Hoyt, DHS, "Critical Infrastructure Protection," Presentation to NSF Workshop on Critical Infrastructure Protection (CIP) for SCADA and IT Systems , 19 October 2003.

SCADA Vulnerabilities

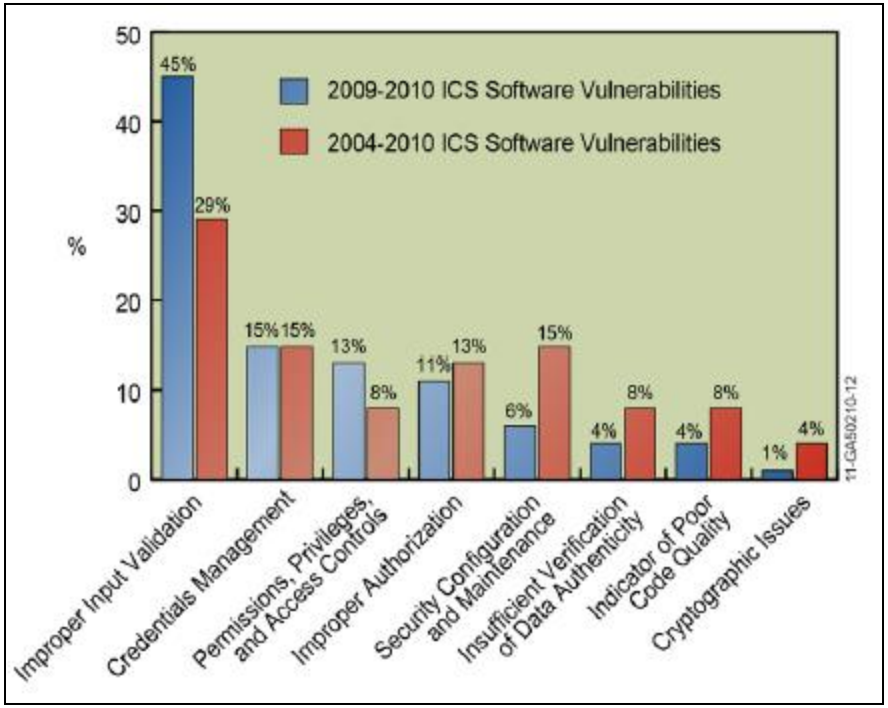
"…On Thanksgiving Day …, Aaron Portnoy, the VP of research at Exodus Intelligence, was able to uncover no fewer than 23 vulnerabilities in SCADA systems in just a few hours. The first exploitable zero-day took a mere seven minutes to discover. "I had a morning's worth of time to wait for a turkey to cook, so I decided to take a shot at finding as many SCADA zero day vulnerabilities as possible," he explained. "For someone who has spent a lot of time auditing software used in the enterprise and consumer space, SCADA was absurdly simple in comparison."

http://www.infosecurity-magazine.com/view/31203/another-honeywell-ics-vulnerability-rears-its-head-in-building-control/?goback=.gde_1222087_member_222594055

The above story sums up my observations over 25 years.

SCADA Vulnerabilities are Well Known

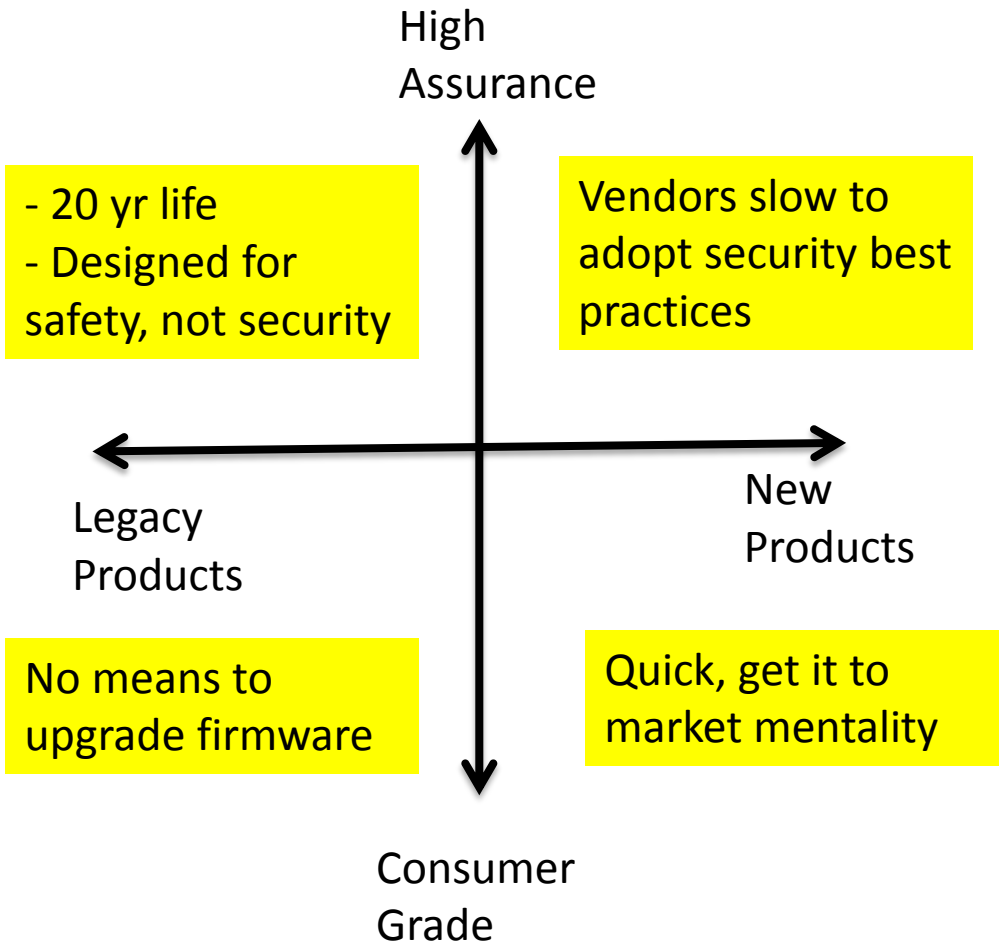
"Current vulnerabilities in ICS product assessments continue to be improper input validation by ICS code. Through bad coding practices and improper input validation, access can be granted to an attacker allowing them to have unintended functionality or privilege escalation on the systems"



DHS, *Common Cybersecurity Vulnerabilities in Industrial Control Systems*, May 2011, Figure 3.

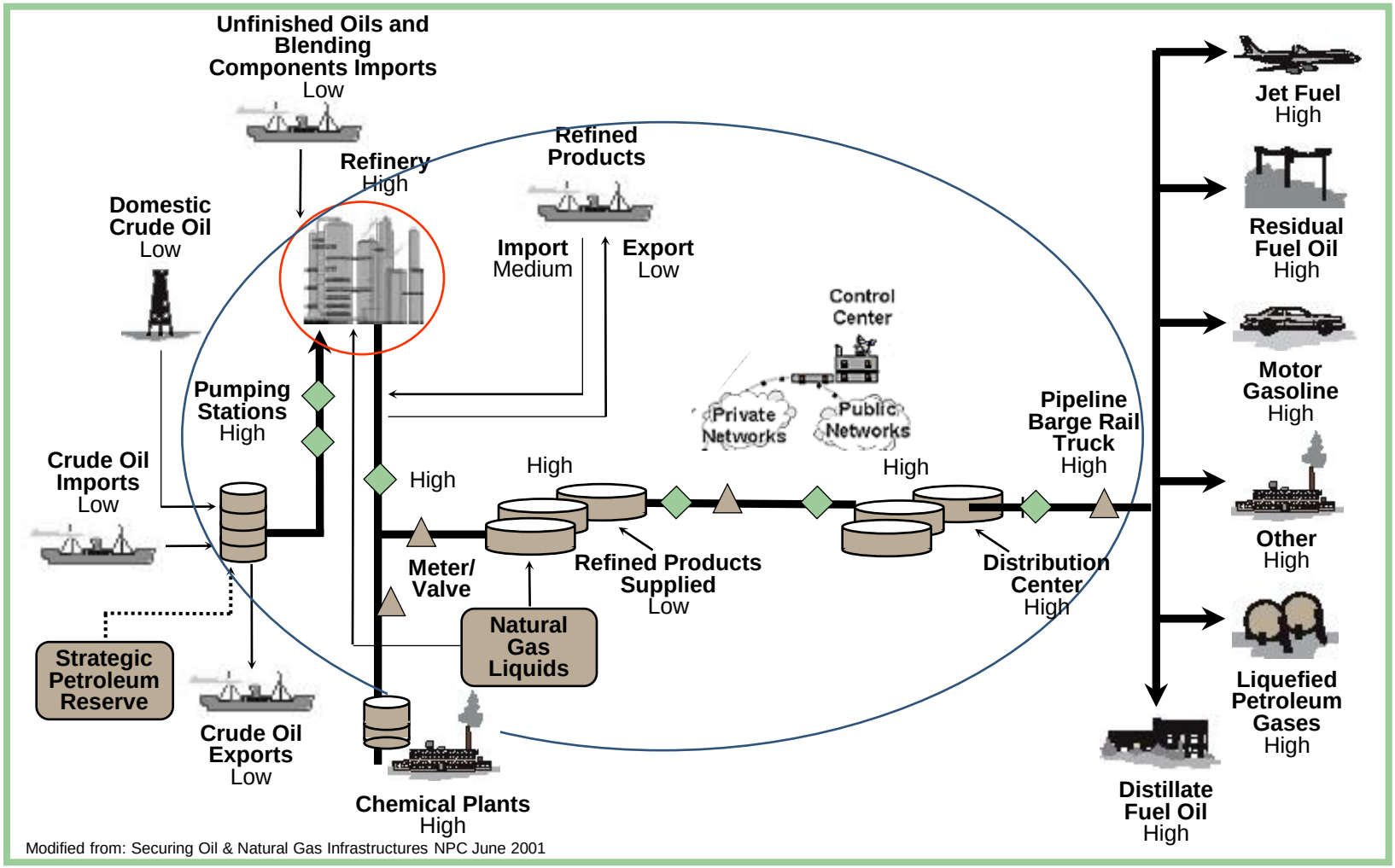
SCADA: Why is Security so Difficult?

The security vulnerabilities for the entire class of industrial control are broadly known, and have been known for two decades.



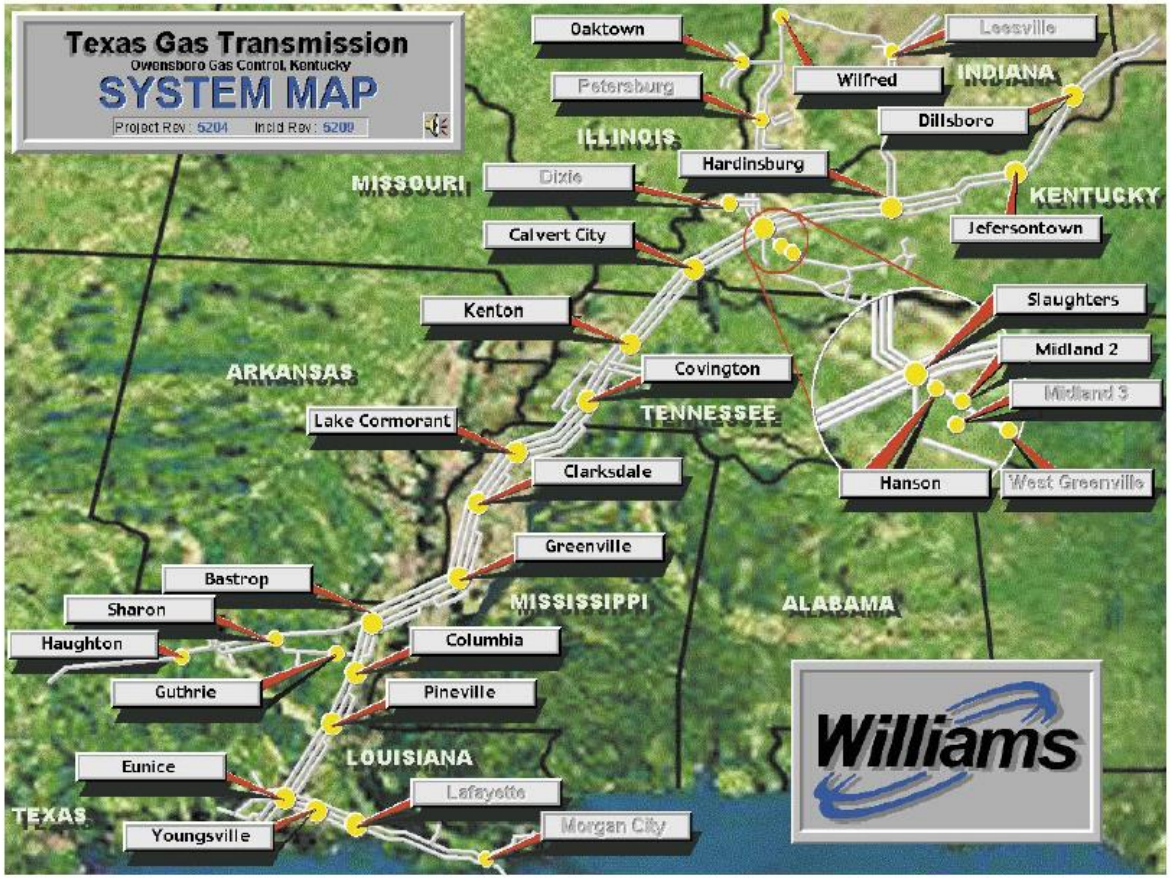
Overarching issue: New technologies are being integrated with out consideration for system security. Wireless, cloud, cell phones, IP enabled components …

Example: Oil Infrastructure



SCADA controls everything in the oil infrastructure.

Example of Modern Gas Pipeline Control



Texas Gas pipeline system

- 6,200 miles of pipe
- 26 compressor stations
- 7 states - 500,000 customers
- Monitor 68,480 control points
- Citect SCADA @ each station,
  - single sever architecture,
  - 384Kbs WAN Fractional T1
  - 30 day historical data logging
  - Operation, flow, temperature, engine parameters, pressure
- Central 24/365 operations center.
  - Located Owensburg
  - Central data logging
- Web based business network interfaces with Central via proxy server
- Single maintenance shift at most stations
- Part time staff at smaller compressor stations

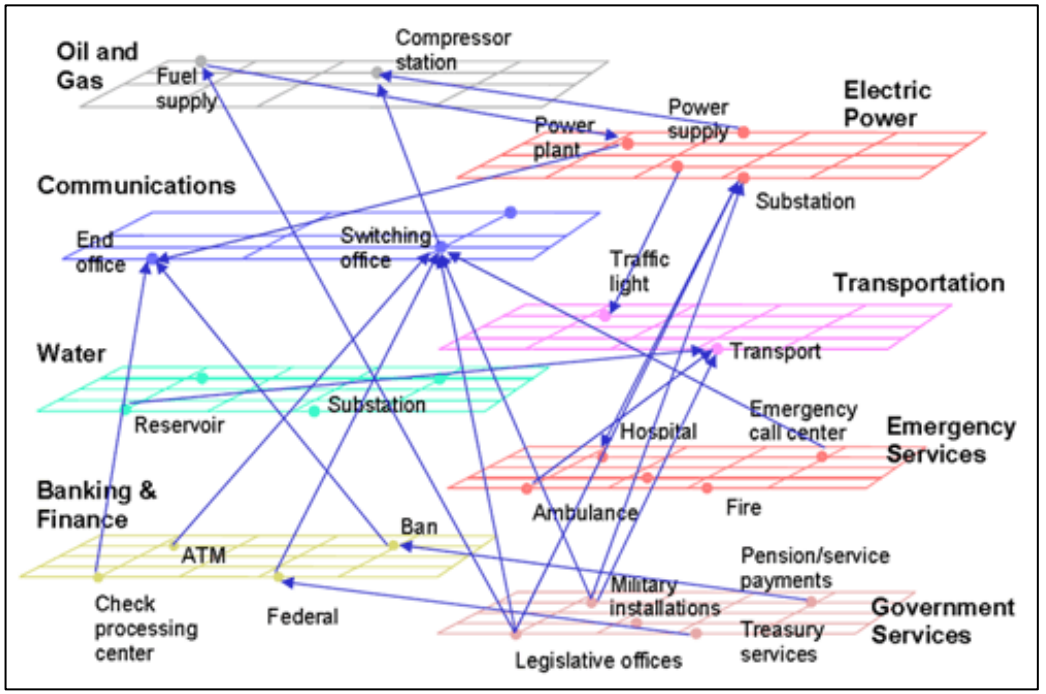
<<http--www.citect.com-__data-page-1806-Texas_Gas_Citect_Case_Study.pdf.url>

Large scale critical infrastructure has adopted broadband.

Interdependence: Literally Everything

How bad actors view infrastructure

- Use infrastructure as a weapon
  - Stalk target on road
- Use infrastructure to stage or deliver an attack
  - Deliver malware to disable vehicle
- Use infrastructure to support an attack
  - Take down emergency communication before the attack



http://transition.fcc.gov/pshs/techtopics/techtopics19.html

You have what they want.

WHAT THE BAD GUYS WANT

What the Bad Guys Want

- **Criminal and Nation-State exploitation for financial gain, collection of intellectual property, and exploitation of U.S. infrastructure is where the "game" will be played over the next 5 years.**
- **Cyber space is a level playing field.**
- **The adversary is good at the "game", adapts quickly, and is in it for financial gain and positioning for the future.**

"The Nation-States will attack and they will succeed! Put plans in place to mitigate the damage." FBI Section Chief Peter Trahon, Section Chief of the Cyber National Security Section

They Want Your Data & Money

"…U.S. companies lose some $250 billion to intellectual property theft every year…. Internationally, $114 billion was lost to cybercrimes, but that number could be as high as $388 billion if the value of time and business opportunities lost is included. McAfee, the computer software and security company, gives an even higher number, saying $1 trillion is spent globally in remediation efforts." – Gen. Keith Alexander, National Security Agency Director

"He who controls/owns the data wins the game!"

What do the Bad Guys Like? Your Creds

Billions of Digital Credentials Stolen (August 2014)

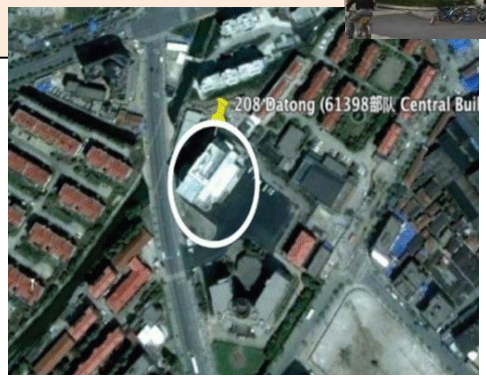
A group of Russian thieves has collected a stash of Internet account credentials: 1.2 billion user name and password combinations and 500 million email addresses. The data were taken from more than 420,000 websites.

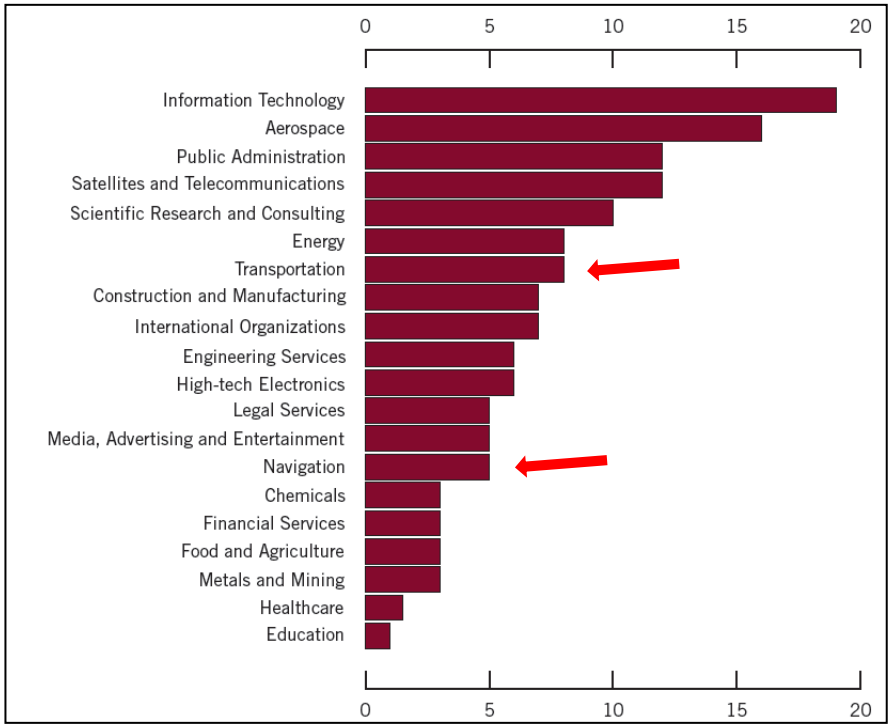
http://krebsonsecurity.com/2014/08/qa-on-the-reported-theft-of-1-2b-email-accounts/]

http://www.nytimes.com/2014/08/06/technology/russian-gang-said-to-amass-more-than-a-billion-stolen-internet-credentials.html?

Nation States: Want Technology & Know-How

"The sheer scale and duration of sustained attacks against such a wide set of industries from a singularly identified group based in China leaves little doubt about the organization behind APT1. …"





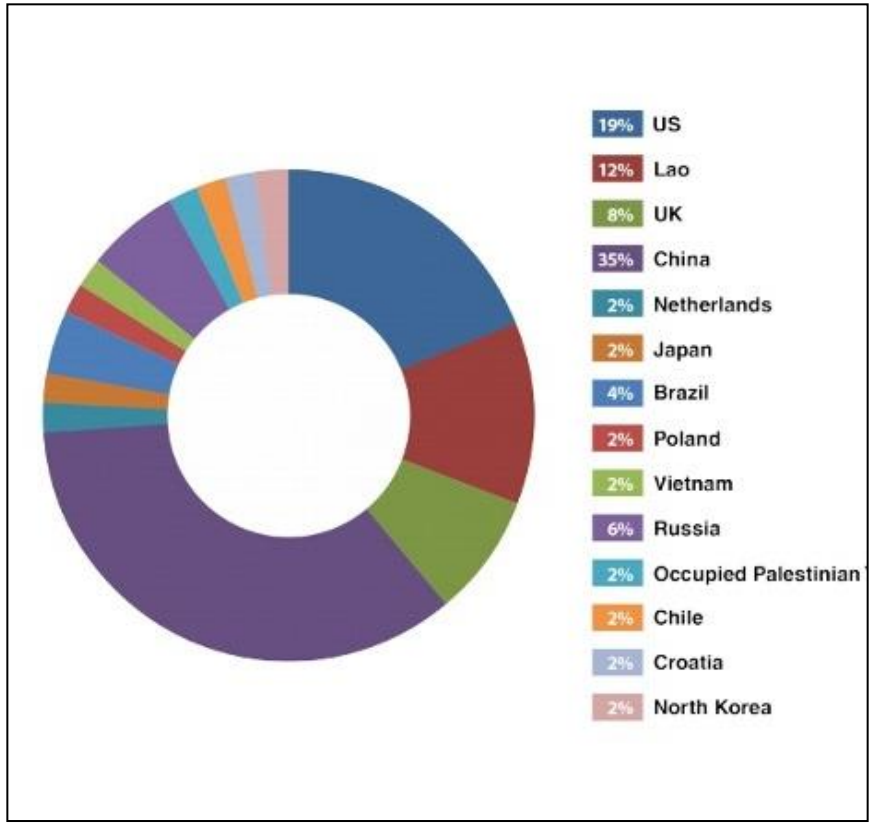
"Our observations confirm that APT1 has targeted at least four of the seven strategic emerging industries that China identified in its 12th Five Year Plan"

MANDIANT: APT1 Exposing One of China's Cyber Espionage Units

Nation States & Criminals Are Looking

ICS Honeypot experiment: Two dummy industrial control systems (ICS) and one real one to the Internet

- First attack in 18 hours.
- 12 unique attacks that could be classified as "targeted,"
- 13 attacks repeated by same actors.
- Attackers used automated tools that search out industrial.
- Hackers probed the site and manipulate devices if possible.
- Attacks included modifying settings to change water pressure and stop the flow on a water pump.
- Attacks used techniques specific to industrial control systems.
- Attacks involved sending emails to the administrator address.



www.waterworld.com/articles/iww/print/volume-13/issue-3/columns/industrial-control-systems-targeted-by-hackers.html?goback=.gde_1222087_member_251346148

Capabilities of Criminal & Nation State

Anatomy of Criminal/Nation State Attack

1. Establish an attack infrastructure (tools, methods, techniques)
2. Conduct recon on target
3. Draft a spear-phishing email
4. Compromise the end-point
5. Obtain valid credentials
6. Map out victim's network
7. Set up hidden directory for data capture
8. Compress / encrypt data for transfer

Source: FBI Section Chief **Peter Trahon,** Cyber National Security Section, 13 March 2012, MN InfraGard meeting on Electronic Espionage

"External agents have created economies of scale by refining standardized, automated, and highly repeatable attacks directed at smaller, vulnerable, and largely homogenous targets." (Verizon)

"Most of the victims were notified by the USG / FBI" Peter Tahron

Four APT Examples

- Stuxnet
  - Identified June 2010
  - Believed built on the Flame platform
  - Infects by USB drives
- Duqu
  - Identified September 2011
  - Designed to capture key strokes and system information
- Flame
  - Identified May 2012
  - Believed the original malware dates to 2006
  - “Scout” for Stuxnet
  - Largest malware program ever seen (20 MB)
- Red October
  - Discovered October 2012
  - Advanced cyber espionage targeted diplomatic, governmental and scientific research organizations worldwide
  - Operated 6+ years
  - Auto shut-down after discovery

Repurposing of APT Cyber Attacks

BAI – “ Howard, please comment on the repurposing of Duqu, Flame, and Stuxnet by criminal organizations”

HS – “Yes, you are correct. We are seeing a massive reuse of the components of these sophisticated attacks. Once the malware was discovered and dissected, the reuse started in a matter of weeks.”

Howard Schmidt, former Special Assistant to the President and Cyber Security Coordinator, Cyber Security Summit, Oct. 9th 2012

Don’t panic

APPROACH FOR SECURING THE FUTURE

What We Know About Transportation Security

We have established that:

- You can't hide from the problem.
- The vulnerabilities exist and are well known.
- Interdependency exasperates the issues and magnifies the impact.
- The bad actors are exploiting the vulnerabilities for financial gain and espionage.
- Security has the "weakest link in chain" problem.
- Even well run organizations can/will be breached.

Technology is Not the Problem

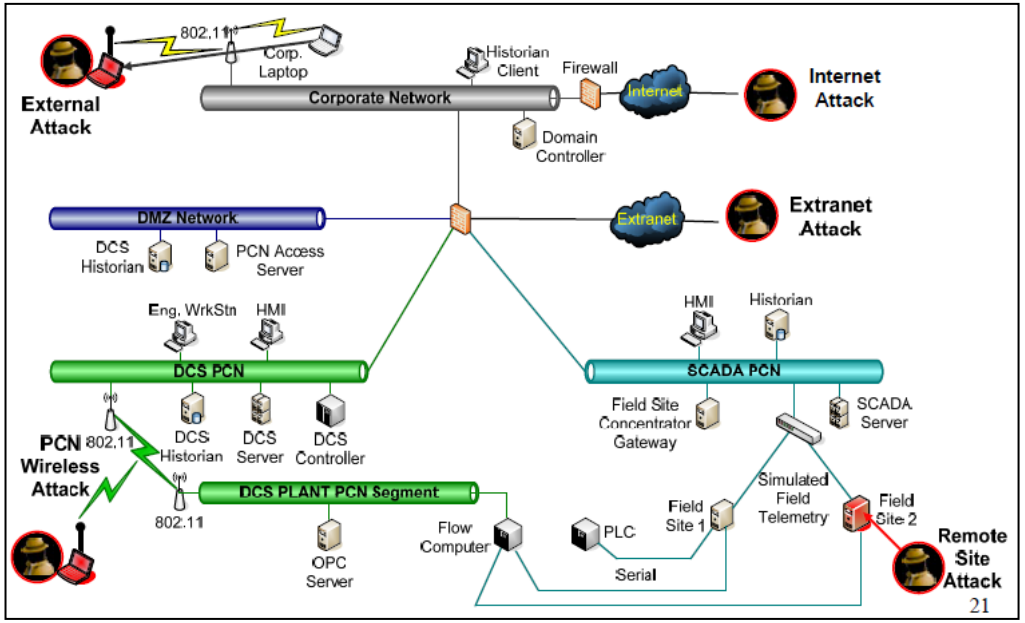
LOGIIC 2007

Standard IT Defenses

- Network Segment Firewalls
- Host Firewalls
- Network Intrusion Detection Systems (IDS)
- Network Devices (switches, routers, wireless devices)

Control System Event Sources

- Standard IT network IDS using signatures for a control system protocol (Modbus)
- Alarms from SCADA and DCS systems
- Alarms from a flow computer



http://www.logiic.org

LOGIIC and other programs show that SOA IT technology can detect and deter attacks in ICS/SCADA systems.

The Security Path Forward

是故勝兵先勝而後求戰，敗兵先戰而後求勝。
Victorious warriors win first and then go to war, while defeated warriors go to war first and then seek to win.

http://en.wikiquote.org/wiki/Sun_Tzu

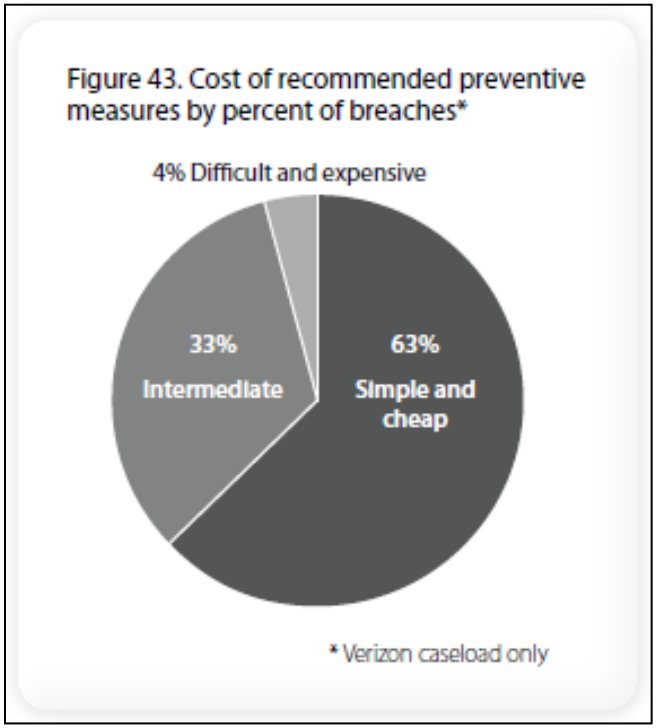
Brian's Opinion: Key Security Policy

- Establish security organization built on clear polices, procedures, best-practices, and trained personnel.
- Procurement:
  - Buy from vendors who "build security in" and deliver in "secure mode".
  - Standard "security language" for RFPs and POs.
- Engineering:
  - Specify only products that are cyber tested and certified.
  - System architecture with focus on security & resilence (network segmentation & controlled access).
- Adopt a "full life cycle view" of security.
  - Strict control and testing before integrating new technology.
  - Protect/harden your legacy systems.

Security is a process, not an end point.

Conclusion – There is Hope

"The latest round of evidence leads us to the same conclusion as before: your security woes are not caused by the lack of something new. They almost surely have more to do with not using, under using, or misusing something old." (Verizon DBR)



(Verizon)

This is not rocket science. However winning will require persistence, alertness, and agility.

Questions?